Published and Copyright (c) 1999 - 2015
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1730 09/29/06

~ Firebee Update, cont. ~ People Are Talking! ~ Apple Squashes Bug!

~ Lenovo Gave Us Crapware ~ Intel Processor Flaw! ~ Intern Hacks Facebook!

~ Kapersky Faked Malware! ~ Destinyâ s Best Weapon! ~ Run Win 10 on Mac!

~ ~ â Hahaâ Has Killed LOL! ~

-* Resident Evil 2 Gets Remake *-
-* Microsoft (Ab)used Personal Data! *-
-* Link Between Violent Games and Aggression *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

First off, apologies to those who usually read each weekâ s web version issue online, or download it to read later. In my attempt to rush last weekâ s issue out the door, I forgot to post the updated issue and appropriate links. I remembered that I hadnâ t done so later in the week but just didnâ t have the time to produce and make them available!

Fast forward to this weekâ s issue, and more troubles! I went to power up my PC to work on the issue this week, but the machine wouldnâ t turn on. For the record, I usually leave my PC on all the time, but last week I shut it down. All of my A-ONE templates and whatever articles Iâ ve accumulated during the week are on that machine. Sure, I have a back-up of most of that stuff on my Mac and a flashcard, but I rely on the PC to put everything together; and then I bring everything over to the Mac for posting and mailing! At the moment, Iâ m not sure how Iâ m going to create my web versions/pages because I rely on an ancient version of Netscapeâ s Composer to create those pages. Now Iâ ll have to see if thereâ s a Mac version of Composer floating around on the web, or try to find something comparable. So, if youâ re looking for the web versions, you may not find them again this week! Sorry!

So, here we are with a â shortenedâ version of the magazine because I â lostâ a number of articles that I saved up for future use; and had planned for this week! The best laid plansâ ƒ Creating this weekâ s issue on the Mac, Iâ m driving blind! I have no idea how this issue is going to look to you - how it will end up being formatted and whatever. On the PC, I have everything set up in an 80-column design using WordPad and NotePad; but on the Mac,

Iâ m using TextEdit and NotePad. Hopefully, there wonâ t be much difference in how you see
your copy of this weekâ s issue. And even more importantly, I hope I either get things
resolved with the PC or be able to find comparable programs on the Mac to make this
â conversionâ as seamless as possible! I truly hate surprises like these!

Until next timeâ ƒ

=~=~=~=

Firebee Update, continued

Last submission I was discussing the issues I was going through with the keyboard, 10MB Hub and the video resolution.´ After E-mailing Mathias Wittau about the monitor I switch monitors again to a Dell 15 inch LCD that had DVI connection so I didnâ t have to use a DVI to VGA adapter.´ I hooked that up and turned the unit on.´ This time the FireBee didnâ t boot into MiNT but into a TOS Boot Menu asking if I wanted TOS for MiNT, EmuTOS, or Plain TOS.´ I chose TOS for MiNT and got only a standard TOS Desktop.´ ´ So I shut down and tried again and the same thing occurred.´ At this point I realized that maybe my Boot Drive C: was corrupt and could no longer boot into MiNT.´ This is the 16GB Compact Flash (CF) card inside the FireBee.

I opened the FireBee and removed the CF Card.´ I have a CF Card reader built in to a Windows Vista PC, but Windows does not allow you to create more than a single partition when working with CF Cards.´ I did insert the CF card into that PC and Windows could not recognize the CF Card.´ At that point I realized I needed another CF Card Reader.´ I went to a local computer store and purchased an IDE to CF Card reader for $14.´ I was hoping for a USB to CF Reader but those were $60 and more.´ ´ I have an old PIII computer that I have various hard drives that I swap in and out depending on what the project is.´ I put in the Linux hard drive and disconnected the CD-ROM drive and attached the CF Card Reader to the CD-ROM IDE cable and attached power.´ I booted the PC with the CF Card attached.´ (Unfortunately when writing this article I could not find the English version of setting up the CF card in time so hereâ s the German page: http://wiki.newtosworld.de/FireBeeCFTutorial.´ (You can always translate the German to English and read further if desired.)´ Under Linux it states to use the GPARTED command.´ My install of Lubuntu did not have GPARTED installed.´ No big deal I would just go to the software manager and install it.´ Unfortunately my install of Lubuntu was too old for any new software to be installed.´ So I went to another machine to download the latest Lubuntu 15.04 http://lubuntu.net/´ Once that was done I burned the ISO to DVD and installed that to the PC.´ Then I could get GPARTED installed.´ Now I can finally see the state of what is on the CF Card.´ The CF card appears to be corrupted and showing nothing at all.´ At this point I´ decided to purchase a new CF Card and leave the original intact to maybe try and figure out what happened to it.´ I purchased a 8GB CF card from a local retailer and attached that to the PC and booted into Linux.´ ´ Basically what the Tutorial states is that with the CF Card you want a minimum of two partitions with the first being made bootable.´ Also the First partition should be 2GB or smaller and FAT16 with the second being FAT32 or EXT2.´ I made the first partition FAT 16 990MB and the remainder of the CF Card the second partition FAT32.´ I made the first partition bootable and shut down.´ Then I went to http://atari.nvg.org/firebee-mint/ and downloaded the FreeMiNT setup for the

FireBee and the updates and followed the instructions as stated on the Web Site. ´ I did these from the Windows Vista PC since now that the CF Card was already prepared the Windows PC was able to work with the CF Card without issue.´ Plus I am more familiar with Windows and the PC was far faster than the PIII is was r unning Linux on.´ After all this effort I installed the freshly prepared CF Car d into the FireBee and turn it on.´ After the TOS Boot Menu I select TOS for Mi NT and Success,´ The FireBee booted into FreeMint!´ ´ I set the video resoluti on to 1024x768x32bit and explored what was on the Drives C: and D:.

After much speculation on what caused the original CF Card to become corrupted I am 95% sure that the card is defective.´ I contacted the manufacturer and they agreed from what trouble shooting I did that the card appeared to be defective to them also.´ I will be sending the card back to the manufacturer for a replac ement this week.´ Yes all this effort appears to have been a lot of hassle but to me I learned a whole lot about the FireBee and setting MiNT up.´ Once runnin g I went and purchased another 8GB CF Card and made a backup of the working card as I had started installing software to the card.´ Then after major changes I will copy the working card to the backup card in case something happens I can re cover much faster.

Lastly any USA Atari Enthusiast who wish to give my FireBee a test drive I will be at the ACEC Swap Meet August 29, 2015 in Columbus Ohio.´ Information on the club and show is here http://www.angelfire.com/oh4/acec/acec.html´ I will have the FireBee setup for users to try out and I will answer any questions the best I can.´ I will also have my Raspberry Pi running Hatari and Aranym for those wh o want to see that in action too.

=~=~=~=

->In This Week’s Gaming Section - Resident Evil 2 Getting Remake!
"""""""""""""""""""""""""""""""" Destinyâ s Best Weapon Is On Sale This Weeke nd!

Link Between Violent Games and Aggression!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

One of the Best Video Games of the â 90s is Getting A Remake

Resident Evil 2, the classic survivalist horror video game, is making a comeback , Capcom announced Wednesday.

The details are hazy at this point, but the remake is being led by Yoshiaki Hira bayashi under Capcomâ s R&D Division 1. Hirabayashi also headed up Capcomâ s r elaunch of original Resident Evil, which came out this year.

Capcom made the announcement in a video on its website.

â Fans have been asking for an RE2 remake for years now, and weâ re happy to f inally confirm one is coming,â the company wrote in the blog announcement. â However, as [Hirabayashi] mentions in the video, youâ re learning this news pra ctically as fast as it happens, so further updates may take some time. Game deve lopment is a long process and the team wants to deliver a remake that lives up t o expectations.â

Gamers Rejoice: Destinyâ s Best Weapon Is On Sale This Weekend

The day has finally come. Xˆ»r, the exotic weapon and armor salesman in Destiny, is selling Gjallarhorn. For those of you who missed purchasing Ice Breaker from Xˆ»r when it was first on saleâ you know, back when strange coins were still s trange and not slowly accumulating into the hundreds in your vault â try not t o miss the boat on this one.

For 17 strange coins youâ ll have the opportunity to buy at least several to ma ke up for its absence from your inventoryâ and Crota hard-mode runsâ for the p ast few months. Unless you already had one, then continue in your apathy.

Now while this may appear to come as literally the best thing ever, we should re serve that feeling of extraordinary bliss. In the Update Preview released by Bun gie on July 16, they stated the intention to nerf Gjallarhornâ s Wolfpack Round s. So for those of us who never had it, at least weâ ll get one thatâ s not as good.

The reason for nerfing it? Apparently everyone was using it and â was so strong that for many people it had become the only answer to getting through tough enc ounters.â Who knew?

Additionally citing that they â strive for Destiny to be a place where a single weapon or strategy does not dictate how, or with whom, you spend your time.â (Maybe if DLCs â okay, every level in the game â werenâ t just the same map s run in reverse Iâ d be inclined to agree with that assessment.)

So at least now while youâ re waiting on your 8-second Ice Breaker cool downs (also to be in the new patch), now you have some time to admire the five Gjallarh orns in your inventory you just bought.

American Psychological Association Affirms Link Between Violent Games and Ag gression

Playing violent video games is linked to increases in aggression and decreases i n sensitivity to aggression, according to a review by the American Psychological Association (APA) of recent research. The review indicated that there is "insuf ficient evidence" about whether playing violent video games can also lead to cri minal violence or delinquency, the APA´ announced today.

The review comes in a´ 49-page report from the´ APA Task Force on Violent Media, which the APA established in January 2013 to review scientific literature publi shed between 2005 and 2013 about the effects of violent video games.

"The research demonstrates a consistent relation between violent video game use and increases in aggressive behavior, aggressive cognitions and aggressive affec

t, and decreases in prosocial behavior, empathy and sensitivity to aggression," the report concludes. The Entertainment Software Association refuted the report in a statement to Polygon, pointing out that the Supreme Court previously dismis sed the supposed link.

Researchers express concerns about APA Task Force on Violent Media
There isn’t enough evidence of a potential link between playing violent games an d committing acts of criminal violence, according to the report, because "very l imited research" exists on that topic, said Mark Appelbaum, PhD, chair of the AP A Task Force, in a press release.

The report notes that "no single risk factor consistently leads a person to act aggressively or violently. Rather, it is the accumulation of risk factors that t ends to lead to aggressive or violent behavior." Playing violent video games is one such risk factor, the report says.

Based on the report, the APA has adopted a new set of policies and recommendatio ns that replaces its 2005´ "Resolution on Violence in Video Games and Interactiv e Media."

In the new document, simply called "Resolution on Violent Video Games," the APA "strongly encourages" the ESRB to update its video game rating system "to reflec t the levels and characteristics of violence in games, in addition to the curren t global ratings." The APA will also endorse the development of "rigorously test ed interventions" that educate children and families about the effects of playin g violent games, and will support further research into the field.

Additional research is necessary to fill gaps in knowledge of the consequences o f playing violent video games, according to the report. The APA Task Force ident ified limitations of the existing body of research such as the effects of playin g violent games on children under the age of 10 â most studies have focused on adolescents and adults â and whether the effects differ between male and fema le individuals.

Appelbaum acknowledged "some variation among the individual studies," but said t hat "a strong and consistent general pattern has emerged from many years of rese arch that provides confidence in our general conclusions."

But the Entertainment Software Association, the trade body representing the U.S. video game industry, disagrees with the APA Task Force’s report. The organizati on slammed the report in a statement to Polygon, saying, "Considering the APA’s long-standing bias against and attacks on video games, this slanted report is no t surprising. Numerous medical professionals, researchers, and courts all debunk the fundamental thesis of their argument."

The ESA went on to cite the Supreme Court’s opinion in Brown v. EMA, the 2011 ca se in which the court decided a California law that banned the sale of violent v ideo games to minors was unconstitutional.

Practicing immoral behavior in a game may make you more morally sensitive, study says "In tearing down similar faulty research, the U.S. Supreme Court specifica lly ruled that ’psychological studies purporting to show a connection between ex posure to violent video games and harmful effects on children do not prove that such exposure causes minors to act aggressively.’ We could not state it better," the ESA said.

Regarding the ESA’s charges of a "long-standing bias" against video games at the APA, it’s worth examining the APA Task Force on Violent Media more closely.

The APA Task Force was created in January 2013, the same month President Barack

Obama suggested further research from the Centers for Disease Control and Prevention into the potential links between video games, "media images" and violence. That call to action followed the December 2012´ mass shooting at Sandy Hook Elementary School in Newtown, Connecticut, in which 20 students and six adult staff members were killed.

In September 2013, a group of nearly 230 academics, researchers and psychologists signed a letter´ expressing concerns about the APA Task Force's review process. The APA's original 2005 resolution came to "several strong conclusions on the basis of inconsistent or weak evidence," according to the signatories of the letter. They continued, "Research subsequent to that 2005 statement has provided even stronger evidence that some of the assertions in it cannot be supported."

Two of the seven members of the APA Task Force, Kenneth Dodge, PhD and Sherry Hamby, PhD, endorsed an amicus curiae brief submitted in favor of upholding the California law in the Brown v. EMA case. The brief came from´ now-disgraced California state Sen. Leland Yee, a well-known crusader against violent video games.

The APA Task Force's review also doesn't include the latest research on violent video games, since the Task Force only examined studies published until mid-2013. A 2014 study led by Matthew Grizzard at the University at Buffalo indicated that practicing immoral behavior in a virtual environment â such as killing someone in a violent video game â could actually lead to an´ increase in prosocial behavior. Contrary to the APA Task Force's report, Grizzard's research found that players would become more sensitive to the moral codes they were violating in the game.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Russian Antivirus Firm Faked Malware To Harm Rivals

Beginning more than a decade ago, one of the largest security companies in the world, Moscow-based Kaspersky Lab, tried to damage rivals in the marketplace by tricking their antivirus software programs into classifying benign files as malicious, according to two former employees.

They said the secret campaign targeted Microsoft Corp , AVG Technologies NV , Avast Software and other rivals, fooling some of them into deleting or disabling important files on their customers' PCs.

Some of the attacks were ordered by Kaspersky Lab's co-founder, Eugene Kaspersky , in part to retaliate against smaller rivals that he felt were aping his software instead of developing their own technology, they said.

"Eugene considered this stealing," said one of the former employees. Both sources requested anonymity and said they were among a small group of people who knew about the operation.

Kaspersky Lab strongly denied that it had tricked competitors into categorizing

clean files as malicious, so-called false positives.

"Our company has never conducted any secret campaign to trick competitors into g
enerating false positives to damage their market standing," Kaspersky said in a
statement to Reuters. "Such actions are unethical, dishonest and their legality
is at least questionable."

Executives at Microsoft, AVG and Avast previously told Reuters that unknown part
ies had tried to induce false positives in recent years. When contacted this wee
k, they had no comment on the allegation that Kaspersky Lab had targeted them.

The Russian company is one of the most popular antivirus software makers, boasti
ng 400 million users and 270,000 corporate clients. Kaspersky has won wide respe
ct in the industry for its research on sophisticated Western spying programs and
 the Stuxnet computer worm that sabotaged Iran’s nuclear program in 2009 and 201
0.

The two former Kaspersky Lab employees said the desire to build market share als
o factored into Kaspersky’s selection of competitors to sabotage.

"It was decided to provide some problems" for rivals, said one ex-employee. "It
is not only damaging for a competing company but also damaging for users’ comput
ers."

The former Kaspersky employees said company researchers were assigned to work fo
r weeks or months at a time on the sabotage projects.

Their chief task was to reverse-engineer competitors’ virus detection software t
o figure out how to fool them into flagging good files as malicious, the former
employees said.

The opportunity for such trickery has increased over the past decade and a half
as the soaring number of harmful computer programs have prompted security compan
ies to share more information with each other, industry experts said. They licen
sed each other’s virus-detection engines, swapped samples of malware, and sent s
uspicious files to third-party aggregators such as Google Inc’s VirusTotal.

By sharing all this data, security companies could more quickly identify new vir
uses and other malicious content. But the collaboration also allowed companies t
o borrow heavily from each other’s work instead of finding bad files on their ow
n.
Kaspersky Lab in 2010 complained openly about copycats, calling for greater resp
ect for intellectual property as data-sharing became more prevalent.

In an effort to prove that other companies were ripping off its work, Kaspersky
said it ran an experiment: It created 10 harmless files and told VirusTotal that
 it regarded them as malicious. VirusTotal aggregates information on suspicious
files and shares them with security companies.

Within a week and a half, all 10 files were declared dangerous by as many as 14
security companies that had blindly followed Kaspersky’s lead, according to a me
dia presentation given by senior Kaspersky analyst Magnus Kalkuhl in Moscow in J
anuary 2010.

When Kaspersky’s complaints did not lead to significant change, the former emplo
yees said, it stepped up the sabotage.

In one technique, Kaspersky’s engineers would take an important piece of softwar
e commonly found in PCs and inject bad code into it so that the file looked like
 it was infected, the ex-employees said. They would send the doctored file anony

mously to VirusTotal.

Then, when competitors ran this doctored file through their virus detection engi nes, the file would be flagged as potentially malicious. If the doctored file lo oked close enough to the original, Kaspersky could fool rival companies into thi nking the clean file was problematic as well.

VirusTotal had no immediate comment.

In its response to written questions from Reuters, Kaspersky denied using this t echnique. It said it too had been a victim of such an attack in November 2012, w hen an "unknown third party" manipulated Kaspersky into misclassifying files fro m Tencent <0700.HK>, Mail.ru and the Steam gaming platform as malicious.

´ ´ ´ The extent of the damage from such attacks is hard to assess because anti virus software can throw off false positives for a variety of reasons, and many incidents get caught after a small number of customers are affected, security ex ecutives said.

The former Kaspersky employees said Microsoft was one of the rivals that were ta rgeted because many smaller security companies followed the Redmond, Washington-based company’s lead in detecting malicious files. They declined to give a detai led account of any specific attack.

Microsoft’s antimalware research director, Dennis Batchelder, told Reuters in Ap ril that he recalled a time in March 2013 when many customers called to complain that a printer code had been deemed dangerous by its antivirus program and plac ed in "quarantine."

Batchelder said it took him roughly six hours to figure out that the printer cod e looked a lot like another piece of code that Microsoft had previously ruled ma licious. Someone had taken a legitimate file and jammed a wad of bad code into i t, he said. Because the normal printer code looked so much like the altered code , the antivirus program quarantined that as well.

Over the next few months, Batchelder’s team found hundreds, and eventually thous ands, of good files that had been altered to look bad. Batchelder told his staff not to try to identify the culprit.

"It doesn’t really matter who it was," he said. "All of us in the industry had a vulnerability, in that our systems were based on trust. We wanted to get that f ixed."

In a subsequent interview on Wednesday, Batchelder declined to comment on any ro le Kaspersky may have played in the 2013 printer code problems or any other atta cks. Reuters has no evidence linking Kaspersky to the printer code attack.

Eugene Kaspersky, chairman and CEO of Kaspersky Lab, listens to a question durin g an interview in New York

As word spread in the security industry about the induced false positives found by Microsoft, other companies said they tried to figure out what went wrong in t heir own systems and what to do differently, but no one identified those respons ible.

At Avast, a largely free antivirus software maker with the biggest market share in many European and South American countries, employees found a large range of doctored network drivers, duplicated for different language versions.

Avast Chief Operating Officer Ondrej Vlcek told Reuters in April that he suspect

ed the offenders were well-equipped malware writers and "wanted to have some fun " at the industry’s expense. He did not respond to a request on Thursday for com ment on the allegation that Kaspersky had induced false positives.

The former employees said Kaspersky Lab manipulated false positives off and on f or more than 10 years, with the peak period between 2009 and 2013.

It is not clear if the attacks have ended, though security executives say false positives are much less of a problem today.

That is in part because security companies have grown less likely to accept a co mpetitor’s determinations as gospel and are spending more to weed out false posi tives.

AVG’s former chief technology officer, Yuval Ben-Itzhak, said the company suffer ed from troves of bad samples that stopped after it set up special filters to sc reen for them and improved its detection engine.

"There were several waves of these samples, usually four times per year. This cr ippled-sample generation lasted for about four years. The last wave was received at the beginning of the year 2013," he told Reuters in April.

AVG’s chief strategy officer, Todd Simpson, declined to comment on Wednesday. Kaspersky said it had also improved its algorithms to defend against false virus samples. It added that it believed no antivirus company conducted the attacks " as it would have a very bad effect on the whole industry."

"Although the security market is very competitive, trusted threat-data exchange is definitely part of the overall security of the entire IT ecosystem, and this exchange must not be compromised or corrupted," Kaspersky said.

Lenovo Used Windows Anti-theft Feature To Install Persistent Crapware

Windows 8 and Windows 10 contain a surprising feature that many users will find unwelcome: PC OEMs can embed a Windows executable in their system firmware. Wind ows 8 and 10 will then extract this executable during boot time and run it autom atically. In this way, the OEM can inject software onto a Windows machine even i f the operating system was cleanly installed.

The good news is that most OEMs fortunately do not seem to take advantage of thi s feature. The bad news is that "most" is not "all." Between October 2014 and Ap ril of this year, Lenovo used this feature to preinstall software onto certain L enovo desktop and laptop systems, calling the feature the "Lenovo Service Engine ."

Lenovo’s own description of what the software did differs depending on whether t he affected system is a desktop or a laptop. On desktops, the company claims tha t the software only sends some basic information (the system model, region, date , and a system ID) to a Lenovo server. This doesn’t include any personally ident ifying information, but the system ID should be unique to each device. Lenovo sa ys that this is a one-time operation and that the information gets sent only on a machine’s first connection to the Internet.

For laptops, however, the software does rather more. LSE on laptops installs the OneKey Optimizer (OKO) software that Lenovo bundles on many of its machines. On eKey Optimizer arguably falls into the "crapware" category. While OKO does do so

me somewhat useful system maintenanceâ it can update drivers, for example â i t also offers to perform performance "optimizations" and cleaning "system junk f iles," which both seem to be of dubious value.

Making this rather worse is that LSE and/or OKO appear to be insecure. Security issues, including buffer overflows and insecure network connections, were report ed to Lenovo and Microsoft by researcher Roel Schouwenberg in April. In response , Lenovo has stopped including LSE on new systems (the company says that systems built since June should be clean). It has provided firmware updates for affecte d laptops´ and issued instructions on how to disable the option on desktops and clean up the LSE files.

The issue was spotted by a poster on our own forums. That poster described some even more undesirable behavior on Windows 7 systems. On those machines, it appea rs that LSE replaces a Windows system file, autochk.exe (which is used for the b oot-time chkdsk filesystem verification and repair process). The bogus autochk.e xe then creates system services that fetch files over unencrypted HTTP.

Lenovo’s own guidance alludes to the overwriting of system files, but it’s not a t all clear how this is happening on Windows 7â the Windows capability to run e xecutables stored in firmware appears to be new to Windows 8 â or why it’s ove rwriting a system file. We’ve asked Lenovo about these issues, but the company m erely referred us to its statement announcing the discontinuation of LSE and the availability of removal tools. (We suspect that the system in question has more than one way of injecting software into Windows, but more on this shortly.)

In the light of Schouwenberg’s bug report, Microsoft recently updated its guidan ce for the´ this facility´ to note that software injected in this way should be written to be secure and that insecure programs are liable to be treated as malw are. As for the feature itself, that remains a part of Windows.

And in its own awful way, it’s a feature that makes sense. The underlying mechan ism is simple enough; the firmware constructs tables of system information when the machine boots. The operating system then examines these tables to, for examp le, learn what hardware is installed in the machine and how it is connected. Thi s is all governed by a specification called ACPI, Advanced Configuration and Pow er Interface. Microsoft defined a new ACPI table, the Windows Platform Binary Ta ble (WPBT), that contains information about a firmware-embedded executable. When it boots, Windows looks for a WPBT. If it finds one, it copies the executable o nto the filesystem and runs it.

The primary purpose of WPBT is the automatic installation of anti-theft software . This kind of software typically does a couple of things that require online co nnectivity: it can phone home to check if it’s been reported stolen (and brick o r otherwise disable itself if it has), and it can phone home to simply report wh ere it is to aid recovery of lost or stolen hardware.

It’s reasonably common (though by no means universal) for stolen hardware to hav e its disk wiped, thereby removing any anti-theft software and limiting the chan ce of recovery. WPBT provides a solution: even if the disk is wiped and the oper ating system reinstalled, the firmware can re-establish the software and report that the laptop was stolen.

Believe it or not, this is one of the less invasive anti-theft techniques in use . Anti-theft system LoJack (also known as Computrace) is widely found on busines s-oriented laptops (including some models from Lenovo). LoJack also injects itse lf into the operating system even after a clean installation, but the way it doe s so is rather more underhanded: it includes BIOS code that directly modifies Wi ndows system filesâ including autochk.exe. Our guess is that LSE uses a similar technique to install itself when booting old operating systems like Windows 7,

explaining the overwritten file that our forum poster observed.

In the context of anti-theft, this kind of capability makes sense and is arguably even desirable. The owner of a system should have the power and authority to establish robust protection in the case of theft. LoJack firmware, for example, traditionally ships in a "disabled" state and requires user intervention to enable. But a manufacturer using an anti-theft technique to install crapware feels like an abuse of the capability, especially as LSE was turned on by default.

Lenovo did include a firmware option to disable LSE, though we've seen one report that a system was showing LSE-like behavior but lacked the option to disable it.

It's not clear which other PC manufacturers have taken advantage of the WPBT capability, or in what capacity they've used it. The company that makes LoJack provides a lengthy list of systems that include its firmware, and most or all of them likely use this system. In the meantime, we'd recommend that users of affected systems (a full list of desktops can be found here and laptops here) update their firmware to remove LSE and then run Lenovo's LSE removal tool to clean the files from their disk.

Apple Squashes Serious Security Bug With Update to Mac OS X

Apple has fixed a bug in its desktop operating system that could have given hackers access to the entire OS.

Released on Thursday, Mac OS X 10.10.5 resolves scores of holes and technical glitches. But one serious bug in particular was squashed along with the rest. Known as DYLD, this vulnerability in Appleâ s OS X was considered serious because it enables hackers to remotely run a program on a Mac using administrator rights, which opens up wide access to the entire operating system. The vulnerability had already been exploited â in the wild,â or in the real world, according to the Guardian, with at least one adware installer taking advantage of it.

The Mac OS has long enjoyed a reputation as more secure than Windows. But just like Microsoft, Apple has to do its fair share of patching with regular updates and bug fixes. The latest update resolves more than 100 different bugs affecting Bluetooth, QuickTime, the Mac OS X kernel, the Macâ s Notification Center and other features. In the past, Apple has sometimes been slow about patching individual bugs, whereas Microsoft rolls out a series of patches on a monthly basis through its Patch Tuesday program.

Appleâ s details on the bug fix, which is available for OS X Yosemite versions 10.10 through 10.10.4, said that with the vulnerability, â a local user may be able to execute arbitrary code with system privileges.â Apple noted that the problem was due to a â path validation issueâ in DYLD and that the issue was addressed through â improved environment sanitization.â Apple did not immediately reply to CNETâ s request for a laymanâ s explanation of these terms.

The DYLD bug was first reported by security researcher Stefan Esser. In a tweet posted late Thursday, Esser said: â Hmm so Apple released 10.10.5 fixed some bugs and made another security problem worse than before.â Esser didnâ t reveal which security problem was allegedly made worse. But he reportedly has advised Mac users not to uninstall his SUIDGuard kernel extension, which guards against attacks that take advantage of the DYLD hole, according to security news site SecurityWeek.

Researcher Exploits Decades-old Flaw in Intel Processors To Access Protected Resources

Decades of changes to x86, Intel’s ubiquitous line of PC processors, have left a labyrinth of forgotten backdoors into privileged access modes, warned independent security researcher Christopher Domas here on Thursday at BlackHat.

Lost in the years of x86 architecture improvements and patches, there is a design flaw that has gone unnoticed, according to Domas.

The flaw lies in the privilege levels that developed in the x86 architecture. The privilege levels originally included only Ring 0 through 3, but then negative rings were added, Domas explained. Eventually, Ring -2, where the system management mode was located, became a "dumping ground" for a lot of things.

"We dumped platform security into system management mode. Why not? Platform security is really, really important and Ring 0 could be compromised. If you put platform security into Ring -2, you don’t have to worry about Ring 0 compromises," he explained.

"But this opened up a Pandora’s Box for what system management mode could do. It is now in charge of an alarming number of very important things for the processor," he added. "Ultimately, Ring -2 is in control of the processor."

Exploiting this Ring architecture, Domas and his team developed a proof-of-concept universal privilege escalation attack. The researchers were able to demonstrate how to jump malware from the Ring 0 into the deepest realms of the processor, Ring -2.

Domas performed this hack with an architectural zero-day vulnerability built into the silicon itself, directed against a vulnerable string of code running on every system with an Intel processor. This enabled Domas’s team to gain authorized access to the sensitive system resources.

Microsoftâ s New Small Print â How Your Personal Data Is (Ab)used

Microsoft has renewed its Privacy Policy and Service Agreement. The new services agreement goes into effect on 1 August 2015, only a couple of days after the launch of the Windows 10 operating system on 29 July.

The new â privacy dashboardâ is presented to give the users a possibility to control their data related to various products in a centralised manner. Microsoftâ s deputy general counsel, Horacio Gutierrez, wrote in a blog post that Microsoft believes â that real transparency starts with straightforward terms and policies that people can clearly understandâ . We copied and pasted the Microsoft Privacy Statement and the Services Agreement into a document editor and found that these â straightforwardâ terms are 22 and 23 pages long respectively. Summing up these 45 pages, one can say that Microsoft basically grants itself very broad rights´ to collect everything you do, say and write with and on your devices in order to sell more targeted advertising or to sell your data to third parties. The company appears to be granting itself the right to share your data either with your consent â or as necessaryâ .

A French tech news website Numerama analysed the new privacy policy and found a number of conditions users should be aware of:

By default, when signing into Windows with a Microsoft account, Windows syncs so me of your settings and data with Microsoft servers, for example â web browser history, favorites, and websites you have openâ as well as â saved app, websi te, mobile hotspot, and Wi-Fi network names and passwordsâ . Users can however deactivate this transfer to the Microsoft servers by changing their settings.

More problematic from a data protection perspective is however the fact that Win dows generates a unique advertising ID for each user on a device. This advertisi ng ID can be used by third parties, such as app developers and advertising netwo rks for profiling purposes.

Also, when device encryption is on, Windows automatically encrypts the drive Win dows is installed on and generates a recovery key. The BitLocker recovery key fo r the userâ s device is automatically backed up online in the Microsoft OneDriv e account.

Microsoftâ s updated terms also state that they collect basic information â fr om you and your devices, including for example â app use data for apps that run on Windowsâ and â data about the networks you connect to.â

Users who chose to enable Microsoftâ s personal assistant software â Cortanaâ have to live with the following invasion to their privacy: â To enable Cortan a to provide personalized experiences and relevant suggestions, Microsoft collec ts and uses various types of data, such as your device location, data from your calendar, the apps you use, data from your emails and text messages, who you cal l, your contacts and how often you interact with them on your device. Cortana al so learns about you by collecting data about how you use your device and other M icrosoft services, such as your music, alarm settings, whether the lock screen i s on, what you view and purchase, your browse and Bing search history, and more. â But this is not all, as this piece of software also analyses undefined â sp eech dataâ : â we collect your voice input, as well your name and nickname, yo ur recent calendar events and the names of the people in your appointments, and information about your contacts including names and nicknames.â

But Microsoftâ s updated privacy policy is not only bad news for privacy. Your free speech rights can also be violated on an ad hoc basis as the company warns:

â We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in pri vate folders), when we have a good faith belief that doing so is necessary toâ ,´ for example, â protect their customersâ or â enforce the terms governing´ the use of the servicesâ .

So much for clearly understandable and straightforward terms of service.

Microsoft Privacy Statementâ ¤https://www.microsoft.com/en-us/privacystatement/d efault.aspx

Microsoft Services Agreementâ ¤https://www.microsoft.com/en-gb/servicesagreement /default.aspx

Windows 10, Microsoft and your personal data: what you need to know (only in Fre nch, 11.06.2015)â ¤http://www.numerama.com/magazine/33357-windows-10-microsoft-e t-vos-donnees-privees-ce-que-vous-devez-savoir.html

Microsoft provides privacy dashboard ahead of Windows 10 launch (04.06.2015)â ¤h ttp://www.pcworld.com/article/2932132/microsoft-provides-privacy-dashboard-ahead

-of-windows-10-launch.html

Harvard Student Loses Facebook Internship for App Exploiting Messenger’s Privacy Flaws

A Harvard University student says he lost his internship at Facebook after he launched a browser application that exploited privacy flaws on its mobile messenger.

Aran Khanna’s app Marauder’s Map, named after the magical map of the Harry Potter series, showed that users of Facebook Messenger could pinpoint the exact locations of people they were talking to.

Khanna posted the app from his dorm room in May and tells Boston.com 85,000 people downloaded it.

Facebook asked Khanna to disable it. A week later, Facebook released a Messenger app update addressing the flaw that a company spokesman said had been in the works for months.

Khanna received a call from Facebook telling him the company was rescinding his internship offer because he violated the Facebook user agreement.

Facebook itself was launched from a Harvard dorm room in 2004.

You Can Now Run Windows 10 on Your Mac

Thanks to the new Boot Camp 6 update, you can now run Windows 10 on your Mac. Boot Camp, a program that allows users of Intel-based Macintosh computers to run the Microsoft Windows XP operating system, was revealed to be updated in a new support document on Appleâ s website.

MacRumors reports â the update is still propagating and is not yet available for OS X,â however some MacRumors members â have noted the update is available within Windows partitions in Boot Camp.â

As of now, it appears this update will not be supported on Macs pre-2012 or on Macs not operating on OS X Yosemite â the full list of compatible Mac models can be found here.

The new Boot Camp 6 update also supports the following Mac features in Windows 10: USB 3, USB-C, Thunderbolt, built-in SD or SDXC card slot, built-in or USB Apple SuperDrive, and your Apple keyboard, trackpad, and mouse.

Windows 10 is a free update for existing Windows users, but youâ ll need to purchase either the $199 Windows 10 Pro or $119 Windows 10 Home if youâ re a new user.

’Haha’ Has Killed ’LOL,’ Says Facebook

If you still â lolâ at jokes online then you might be in the minority. A new

report from Facebook into how users express laughter shows that â hahaâ and its variants are by far the most common terms used on the social network. They accounted for 51.4 percent of mirth in the anonymized comments and posts looked at by Facebookâ s data team, with´ laughter emoji claiming 33.7 percent, and â heheâ and its cognates 13.1 percent. The once-mighty â lolâ only appeared in 1.9 percent of the text sampled by Facebook â a pretty staggering fall for an expression that was once synonymous with online txt speak.

Although not surprising for such a venerable term, â lolâ proved slightly more popular with older users. Differences between generations were not heavily pronounced, but it was emoji that were most popular with users with the youngest median age, while â haha,â â hehe,â and â lolâ were favored by progressively older individuals. The data also showed that emoji were more popular among female users, with â hahaâ showing a small male bias, and â heheâ distributed nearly evenly among the genders. Not may people were regular chortlers though: in the weekâ s worth of data Facebook looked at, 46 percent of those that laughed in the seven days did so only once, with the vast majority â 85 percent â laughing fewer than five times.

Facebookâ s data team also examined how users deployed variants of these laughter terms, looking at whether they heheâ d more than they hehehehehâ d, for example. An´ article in The New Yorker that inspired Facebookâ s analysis suggested that we use â ha"s and "he"s as building blocks, adding up these lexical units to convey everything from polite recognition ("haâ) to no-really-Iâ m-going-a-bit-mad-with-laughter (â hahahahahahahahaâ). Although interpretation of these different strings can be quite subjective, Facebookâ s data showed that even letter counts were more common than odd ones, suggesting that we do indeed stack up these two-letter phonemes like Lego bricks.

As Facebookâ s researchers´ explain: â The most common are the four-letter hahas and hehes. The six-letter hahaha is also very common, and in general, the haha-ers use longer laughter. The haha-ers are also slightly more open than the hehe-ers to using odd number of letters, and we do see the occasional hahaas and hhhaaahhhaas. The lol almost always stands by itself, though some rare specimens of lolz and loll were found. A single emoji is used 50 percent of the time, and itâ s quite rare to see people use more than five identical consecutive emoji.â However, Facebookâ s data scientists should probably look at Instagram, where long strings of´ Face With Tears Of Joy emoji are more common. And judging by the´ demographics of the two social networks, this is how laughter online is likely to look in the future.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of

Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.